Lampi di Cassandra/ iNsecurity

(332)—Una storia di phishing, altruismo e buona volontà; chissà poi come sarà andata a finire. E chissà come andrebbe a finire oggi

---

Lampi di Cassandra/ iNsecurity

Figure 1:

(332)—Una storia di phishing, altruismo e buona volontà; chissà poi come sarà andata a finire. E chissà come andrebbe a finire oggi

19 settembre 2014—Supponiamo che riceviate la prova che qualcuno, non una famosa e sexy attrice ma un signore con tanto di nome e cognome, sia oggetto di un attacco del suo account cloud. Voi cosa fareste?

Il "*bruteforce*", che è un modo molto più raffinato per dire "**indovinare la password**", resta uno dei vettori di attacco più efficaci contro i sistemi telematici.
Avrete certamente letto fino alla nausea dell' "affaire" nato dalla pubblicazione di selfie piccanti di note attrici, cantanti e modelle.
I dettagli dell'accaduto in questa sede ci interessano poco, la marca degli smartphone anche meno, ma il cambiamento rispetto al famoso caso di Cappuccetto Scarlatto è molto importante.

Infatti nel caso dell'attrice Scarlett Johansson è provato che fu il telefono in quanto tale ad essere violato con mezzi informatici da un singolo cracker. Un attacco classico, come a qualunque server degli anni passati, sofisticato e fatto a mano.

La questione dei selfie piccanti è completamente diversa, perché pare oramai assodato che non i

telefoni ma i loro backup nel cloud siano stati attaccati, e non con mezzi manuali ma automatici, forse addirittura botnet.

Questo è stato reso possibile dal fatto che le credenziali da offrire per accedere alla "nuvola" (in questo come in altri casi) è semplicemente un nome utente (spesso un indirizzo di posta) ed una password scelta dall'utente (quella con cui acquistava musica).

Ed è perfettamente inutile difendere il terminale (lo smartphone) con un lettore biometrico quando l'accesso a tutte le informazioni che contiene può essere fatto via internet, semplicemente indovinando una password debole con i consueti attacchi a dizionario.

Ora che il problema ha raggiunto i media, lo stesso Tim Cook si è precipitato a garantire la massima attenzione all'argomento, e l'introduzione di una autenticazione a due fattori.

Il mio problema è che hanno iniziato ad arrivarmi messaggi fake che pretendono di essere della Apple (molto ben fatti) e che chiedono ad un quasi mio omonimo, identificato con nome e cognome (il signor Marco C……ia) di autenticarsi al suo account iCloud.

L'indirizzo di posta è il mio perché sintetizzato, tra i tanti tentativi che un bot compie durante un bruteforce, formandolo con nome e l'iniziale del cognome, usando il nome di dominio uguale al nome utente e come TLD quello della nazionalità del bersaglio.

Insomma, il signor M.C. di cui sopra è quasi certamente uno dei tanti a cui stanno cercando di rubare i backup, le foto e quant'altro. E probabilmente non ci sono ancora riusciti …

Ora è brutto sapere che i ladri stanno tentando di scassinare la porta di casa di qualcuno di cui sapete nome e cognome, anche se è un perfetto sconosciuto. Il tentativo di identificare e scrivere direttamente alla persona può portare ad ad equivoci, al rischio di essere scambiati per dei cattivi, per degli ingegneri sociali, o nella migliore delle ipotesi di essere ignorati. Infatti, nessuna risposta. Ma forse non era l'M.C. giusto.

Poiché ad onor del vero il sito del noto produttore fornisce anche a non clienti la possibilità di porre domande (cosa rara ed apprezzabile), ed addirittura di richiedere un contatto telefonico su appuntamento, potrei provare tramite loro.

Povero signor M.C.. Su, avanti con la buona azione!

Riempio il form, chiedo il contatto per l'indomani e…. miracolo, all'ora spaccata un'operatrice italiana (o che parla perfettamente l'italiano) mi chiama al cellulare chiedendo gentilissimamente di cosa ho bisogno.
Tanto di cappello all'help desk del noto produttore.

Le spiego che io personalmente non ho bisogno di niente, ma che il loro cliente signor M.C. è attualmente vittima di un tentativo di attacco come quello finito sui giornali, e che quindi sarebbe opportuno avvertirlo di cambiare la password con una molto robusta nel caso non ce l'avesse già, e di togliere da iCloud i dati sensibili che ci fossero finiti.
Si fa spiegare tutto due volte, gentilissima sembra che abbia capito la questione; vengo congedato con la promessa di essere richiamato.

Ovviamente nulla.

Nei giorni successivi continuano però ad arrivarmi altre mail, sempre col mio indirizzo di posta, sempre con il nome di questa persona.
Riproviamo, altro form, altra richiesta di contatto, altra telefonata puntualissima, altra signorina gentilissima a cui racconto la storia, con l'aggiunta dei dati della precedente chiamata a cui non era stato dato seguito.

Con una certa sorpresa da parte mia mi viene stavolta risposto che per risolvere il "mio" problema dovevo mandare una richiesta scritta od utilizzare un altro link perché "loro" non potevano fare niente.
Con tono giustificatamente seccato faccio presente con non si trattava di un "mio" problema, ma di un "loro" problema, di un loro cliente e quindi di tutta l'organizzazione, iniziando da lei fino ad arrivare al CEO (che tra l'altro aveva appena rilasciato la dichiarazione suddetta).

Risposta ripetuta tal quale. Mi limito perciò a comunicare che la mia buona volontà si è esaurita, e che tutto quello che mi rimane è raccontare la storia.
Gentilissimi saluti, e dopo pochi minuti mi viene spedita una mail con un link generico e del tutto inutile.

La morale della storia?

Pur esistendo mezzi e buona volontà, senza un'organizzazione orientata al cliente e reattiva ai problemi di sicurezza, soprattutto a quelli semplici da contrastare, i clienti non vengono aiutati, sono abbandonati a sé stessi.

E' inutile che i CEO promettano miracoli crittografici, quando le serrature dei servizi sono ridicolmente semplici da aprire, ed irrobustirle subito costerebbe soldi e figuracce. Questa storiella può anche servire come monito per un problema ormai imminente.

Gli standard qualitativi, i modelli organizzativi e gli approcci alla sicurezza degli utenti con cui le aziende più disparate produrranno i pezzi dell'*Internet degli Oggetti* sono di questo tipo, anzi probabilmente ancora inferiori. I rischi per coloro che si credono padroni dei loro Oggetti connessi ad Internet saranno quindi infinitamente maggiori.

Speriamo quindi che il signor M.C. abbia una password robusta, e comunque nessun selfie compromettente sul telefono ….

… dopo quella di fare a meno di qualsiasi "nuvola", è un'abitudine che consiglio caldamente a tutti.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on November 5, 2023.

Canonical link

Exported from Medium on August 27, 2025.